CLAIMS

What is claimed is:

1. An access control list (ACL) validation module for detecting at least one of ACL inconsistencies and redundancies in a network device, said module including decision logic for:

(a) accessing one or more object definitions in the form of one or more ACL rules;

(b) accessing at least one permission flag associated with each ACL rule;

(c) modeling each ACL rule as a geometric figure;

(d) detecting an intersection of each modeled geometric figure; and

(e) generating a binary output based on the intersection of the geometric figures.

2. The module according to claim 1, further including a step of extracting substantially all ACL rules from a configuration database.

3. The module according to claim 1, further including a step of tagging each permission flag as either permit or deny.

4. The module according to claim 1, further including a step of representing each ACL rule in a six-dimensional space.

5. The module according to claim 4, wherein one dimension of said six-dimensional space is defined by an internet protocol.

6. The module according to claim 4, wherein one dimension of said six-dimensional space is defined by a source internet protocol address range.

7. The module according to claim 4, wherein one dimension of said six-dimensional space is defined by one or more source ports.

8. The module according to claim 4, wherein one dimension of said six-dimensional space is defined by a destination internet protocol address range.

9. The module according to claim 4, wherein one dimension of said six-dimensional space is defined by one or more destination ports.

10. The module according to claim 1, including multi-dimensional modeling of each geometric figure in the modeling step.

11. The module according to claim 1, employing at least one of a circle, rectangle and solid as a geometric figure in the modeling step.

12. The module according to claim 1, further including a step of incorporating a status of said permission flag in the modeling step.

13. The module according to claim 1, having a step interpreting the intersection of two or more figures to represent an existence of substantially all partial or total ACL redundancies or inconsistencies.

14. The module according to claim 1, having a step interpreting a non-intersecting figure to represent substantially no partial or total ACL redundancies or inconsistencies.

15. The module according to claim 1, having said output comprise pass or fail.

16. The module according to claim 15, wherein a pass output result is indicative of substantially no intersecting figures.

17. The module according to claim 15, wherein a fail output result is indicative of an existence of substantially all partial or total ACL redundancies or inconsistencies.

18. The module according to claim 1, having said output comprise optimization of an ACL.

19. A configuration validation module for providing compliance verification information on an intended functionality of a network device, said module including decision logic for:

(a) accessing one or more configuration files of the network device;

(b) accessing one or more test files, each test file describing an expected configuration characteristic of the network device;

(c) accessing one or more security policy files, each security policy describing which test to apply on which network device and an expected outcome of each test;

(d) applying one or more test and security policy files to the one or more configuration files; and

(e) generating an output indicative of configuration compliance of the network device.

20. The module according to claim 19, further including a step of extracting substantially all configuration files a database.

21. The module according to claim 19, further including a step of extracting substantially all test files from a database.

22. The module according to claim 19, further including a step of extracting substantially all security policy files from a database.

23. The module according to claim 19, having a step of sequentially executing each test and security policy file on each configuration file, said step of sequentially executing included in the applying step.

24. The module according to claim 19, having a step of executing each test and security policy file on each configuration file for each network device, said step of executing included in the applying step.

25. The module according to claim 19, having said output comprise pass or fail.

26. The module according to claim 19, having said output comprise a security assessment report.

27. The module according to claim 19, further including a step of generating a network device configuration change request.

28. The module according to claim 27, further including a step of transmitting said configuration change request to a trouble-shooting system.

29. A network device security policy module for verifying security compliance of the device's configuration, said module:

(a) accessing one or more configuration files of the network device;

(b) accessing one or more test files, each test file describing an expected configuration characteristic of the network device;

(c) accessing one or more security policy files, each security policy describing which test to apply on which network device and an expected outcome of each test;

(d) executing the test and security policy files on the configuration files; and

(e) generating a security assessment report on the network device.

30. The module according to claim 29, further including a step of generating a network device configuration change request.

31. The module according to claim 30, further including a step of transmitting said configuration change request to a network operator.

32. A network device security policy module for providing security compliance verification on a configuration of a network device, said module:

(a) accessing one or more configuration files of the network device;

(b) accessing one or more test files, each test file describing an expected configuration characteristic, including a security policy characteristic, of the network device;

(c) applying one or more test files to each configuration file of the device; and

(d) generating an output indicative of configuration compliance of the network device.

33. The module according to claim 32, wherein each accessing step includes extracting one or more of said configuration files and said test files from a database.

34. The module according to claim 32, having a step of sequentially executing each test file on each configuration file, said step of sequentially executing included in the applying step.

35. The module according to claim 32, having a step of executing each test file on each configuration file for each network device, said step of executing included in the applying step.

36. The module according to claim 32, having said output comprise pass or fail.

37. The module according to claim 32, having said output comprise a security assessment report.

38. The module according to claim 32, further including a step of generating a network device configuration change request.

39. The module according to claim 38, further including a step of transmitting said configuration change request to a fault management system.

40. A communications network security policy module for verifying configuration compliance of a communications network, said module performing the functions of:

(a) accessing configuration files of substantially all network devices in the communications network;

(b) extracting communications network connectivity information from the configuration files;

(c) manipulating connectivity information by employing at least one of network algorithms, modeling and parsing techniques; and

(d) generating an output indicative of security policy compliance verification of the communications network.

41. The module according to claim 40, performing the extracting step in accordance with a desired communications network.

42. The module according to claim 40, having a step of developing a connectivity database included in the extraction step.

43. The module according to claim 40, further including a step of accessing route cost information associated with each communication link.

44. The module according to claim 40, further including a step of accessing route cost information associated with each network device.

45. The module according to claim 40, having a step of modeling connectivity information of the communications network as a directed graph, included in the manipulating step.

46. The module according to claim 40, having a step of modeling connectivity information of the communications network as an undirected graph, included in the manipulating step.

47. The module according to claim 40, further including a step of generating a communications network configuration change request.

48. The module according to claim 40, said output comprising one or more graph-oriented predicates.

49. The module according to claim 40, further including a step of transmitting said configuration change request to a fault management system.

50. A software system for providing security policy compliance verification on a network device, said software system comprising:

(a) a configuration database including one or more configuration files containing information describing an arrangement of the network device;

(b) a test database including one or more test files containing information describing one or more tests, which express one or more expected characteristics, including one or more security characteristics, of the network device;

(c) a security policy database including one or more security policy files containing information describing which test to apply on which device and an expected outcome of each test; and

(d) a validation engine, which communicates with the configuration, test and security policy databases, for processing information of said configuration, test and security policy databases, and generating an output verifying security policy compliance of the network device.

51. The software system of claim 50, wherein each test is written in any programming language.

52. The software system of claim 50, wherein each test produces a standard header and a standard trailer.

53. The software system of claim 50, said validation engine sequentially applying one or more test files and security policy files to the configuration files.

54. The module according to claim 50, said output comprising one or more graph-oriented predicates.

55. A software system for providing security policy compliance verification on a communications network, said software system comprising:

(a) a configuration database including one or more configuration files containing substantially all connectivity information describing an arrangement of the communications network;

(b) a test database including one or more test files containing information describing one or more tests, which express one or more expected security characteristics, of the network device;

(c) a security policy database including one or more security policy files containing substantially all information describing which test to apply on which device in the network and an corresponding expected result of applying the test on the device; and

(d) a validation engine, in communication with at least one of the configuration, test and security policy databases, for processing information of said configuration, test and security policy databases; and

(e) a parser engine, in communication with the validation engine, for instantiating computations on connectivity information and generating an output indicative of security policy compliance verification of the communications network.

56. The software system of claim 55, wherein each test is written in any programming language.

57. The software system of claim 55, wherein each test produces a standard header and a standard trailer.

58. The software system of claim 55, said validation engine sequentially applying one or more test files and security policy files to the configuration files.

59. The software system according to claim 55, said output comprising one or more graph-oriented predicates.

60. The software system according to claim 55, said output comprising an undirected graph of routing information.

61. The software system according to claim 55, said output comprising a directed graph of routing information.

62. The software system according to claim 55, said output comprising a map of one or more critical points of failure for both network devices and links in the communications network.

63. The software system according to claim 55, further including a connectivity database containing connectivity information of the communications network.

64. A computer readable media encoding instructions for detecting substantially all partial or total inconsistencies or redundancies within an access control list, said media including instructions for:

(a) accessing one or more access control list rules;

(b) accessing at least one permission flag for each rule;

(c) modeling each rule geometrically in accordance with an associated permission flag;

(d) detecting an area of intersection of one or more geometric models of the access control list rules; and

(e) generating an output based on the intersection of one or more geometric models.

65. The media of claim 64, further including an instruction for tagging each permission flag as either permit or deny.

66. The media of claim 64, further including an instruction for multi-dimensional modeling of each geometric figure in the modeling step.

67. The media of claim 64, further including an instruction for employing at least one of a circle, rectangle and solid as a geometric figure in the modeling step.

68. The media of claim 64, further including an instruction of incorporating a status of said permission flag in the modeling step.

69. The media of claim 64, having said output comprise pass or fail.

70. The media of claim 64, wherein a pass output result is indicative of substantially no intersecting figures.

71. The media of claim 64, wherein a fail output result is indicative of an existence of substantially all partial or total ACL redundancies or inconsistencies.

72. The media of claim 64, having said output comprise optimization of an ACL.

73. A computer readable media encoding instructions for diagnosing security policy compliance of a network device, said media including instructions for:

(a) accessing one or more configuration files of the network device;

(b) accessing one or more test files, each test file describing an expected configuration characteristic of the network device;

(c) accessing one or more security policy files, each security policy describing which test to apply on which network device and an expected outcome of each test;

(c) executing the test and security policy files on the configuration files; and

(d) generating a security assessment report on the network device.

74. The media of claim 73, further including instructions for generating a network device configuration change request.

75. The media of claim 74, further including an instruction for transmitting said configuration change request to a network operator.

76. A computer readable media encoding instructions for diagnosing security policy compliance of a communications network, said instructions including:

(a) accessing configuration files of substantially all network devices in the communications network;

(b) extracting communications network connectivity information from the configuration files;

(c) manipulating connectivity information by employing at least one of network algorithms, modeling and parsing techniques; and

(d) generating an output indicative of security policy compliance verification of the communications network.

77. A method for detecting at least one ACL inconsistencies and redundancies in a network device, said method comprising the steps of:

(a) accessing one or more object definitions in the form of one or more ACL rules;

(b) accessing at least one permission flag associated with each ACL rule;

(c) modeling each ACL rule as a geometric figure;

(d) detecting an intersection of each modeled geometric figure; and

(e) generating a binary output based on the intersection of the geometric figures.

78. A method for diagnosing compliance of a security policy of a network device, said method comprising the steps of:

(a) accessing one or more configuration files of the network device;

(b) accessing one or more test files, each test file describing an expected configuration characteristic, including a security policy characteristic, of the network device;

(c) applying one or more test files to each configuration file of the device; and

(d) generating a security assessment report for the network device.

79. A method for diagnosing compliance of a security policy of a communications network, said method comprising the steps of:

(a) accessing configuration files of substantially all network devices in the communications network;

(b) extracting communications network connectivity information from the configuration files;

(c) manipulating connectivity information by employing at least one of network algorithms, modeling and parsing techniques; and

(d) generating a security assessment report on the communications network.